Amendments to the Claims:

This listing of claims replaces all prior versions and listings of claims in the application:

Listing of Claims:

1-30. (Cancelled).

31. (Currently Amended) A method for controlling cryptographic functions of an application program, the method comprising:

accessing a policy file that reflects ~~a state associated with~~ a condition of the policy file and that includes an attribute portion configured to store one or more cryptographic policy attributes and a value portion having one or more attribute values, each attribute value corresponding to a cryptographic policy attribute and indicating whether an application program may use the cryptographic policy represented by the cryptographic policy attribute;

selectively retrieving at least one of encryption information and decryption information from the policy file;

selectively processing the retrieved encryption information and decryption information from the policy file in accordance with a predetermined capability condition; and

providing at least one of allowable encryption levels and decryption levels to the application program.

32. (Previously Presented) The method of claim 31 wherein the policy file comprises a JAVA archive file.

33. (Previously Presented) The method of claim 31 wherein the policy file comprises multiple component files, at least one of the component files storing some of the attribute portions and attribute values.

34. (Previously Presented) The method of claim 33 wherein at least one of the multiple component files is associated with a signature portion including at least one digital

certificate for ensuring that the policy file has not been modified and a signature portion including at least one digital certificate for ensuring that the policy file has not been modified and applying to a particular component file.

35. (Cancelled)

36. (Previously Presented) The method of claim 31 wherein the policy file includes a signature portion including at least one digital certificate for ensuring that the policy file has not been modified.

37. (Previously Presented) The method of claim 36 wherein the signature portion applies to the policy file.

38. (Previously Presented) The method of claim 31 wherein:

each of the cryptographic policy attributes includes an indication of the cryptographic capabilities of the application program, and

each of the attribute values is one of a string, an integer number, and a truth expression.

39. (Previously Presented) The method of claim 38 wherein the truth expression is one of a true flag, a false flag, and a conditional flag.

40. (Currently Amended) An apparatus for controlling cryptographic functions of an application program, the apparatus comprising a processor connected to storage and one or more input/output devices, wherein the processor is configured to:

access a policy file that reflects ~~a state associated with~~ a condition of the policy file and that includes an attribute portion configured to store one or more cryptographic policy attributes and a value portion having one or more attribute values, each attribute value corresponding to a cryptographic policy attribute and indicating whether an application program may use the cryptographic policy represented by the cryptographic policy attribute;

selectively retrieve at least one of encryption information and decryption information from the policy file;

selectively process the retrieved encryption information and decryption information from the policy file in accordance with a predetermined capability condition; and

provide at least one of allowable encryption levels and decryption levels to the application program.

41. (Previously Presented) The apparatus of claim 40 wherein the policy file comprises a JAVA archive file.

42. (Previously Presented) The apparatus of claim 40 wherein the policy file comprises multiple component files, at least one of the component files storing some of the attribute portions and attribute values.

43. (Previously Presented) The apparatus of claim 42 wherein at least one of the multiple component files is associated with a signature portion including at least one digital certificate for ensuring that the policy file has not been modified and the signature portion applying to a particular component file.

44. (Cancelled)

45. (Previously Presented) The apparatus of claim 40 wherein the policy file includes a signature portion including at least one digital certificate for ensuring that the policy file has not been modified.

46. (Previously Presented) The apparatus of claim 45 wherein the signature portion applies to the policy file.

47. (Previously Presented) The apparatus of claim 40 wherein:

each of the cryptographic policy attributes includes an indication of the cryptographic capabilities of the application program, and

each of the attribute values is one of a string, an integer number, and a truth expression.

48. (Previously Presented) The apparatus of claim 47 wherein the truth expression is one of a true flag, a false flag, and a conditional flag.